I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

United States Government Cybersecurity Relationships

MARK D. YOUNG*

"Securing our networks is a team sport."
General Keith B. Alexander, USA
Director, National Security Agency
Commander, United States Cyber Command

I. INTRODUCTION

The United States federal government must strengthen its relationships to better design, build, manage, and defend the information infrastructure on which American society and security now depends. Our lives are now inextricably tied to the information that surrounds us. We use an ever-expanding set of devices to access this information and to create order from the chaotic jumble of facts, figures, downloads, and databases that confront us in our professional and our personal lives.

The overwhelming nature of the information age also challenges traditional governance structures. The federal government finds itself managing its interactions with data that is growing at a significant

* Executive Director, Directorate of Plans and Policy, United States Cyber Command. The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or any part of the U.S. Government. This article is derived entirely from open source material and contains no classified information. It is intended to depict the enduring complexity and range of issues and relationships entailed in organizing cyber security policy and implementation at the federal level, even though the lapse of time between writing and publication will undoubtedly render certain specific details obsolete.

rate. It is responsible for creating, managing, and securing a large portion of the terabytes of information needed to ensure national security, maintain diplomatic relationships with other nations, collect taxes, provide benefits, enforce laws, and the myriad other duties needed for a population of more than 312 million people. Information networks, data storage, and management systems play a role in every function of today's federal government. Driven by the financial and access benefits of information technology, the federal government has become as reliant on information systems as the U.S. population, if not more so.

Because of this reliance on computers for governance, the federal government must ensure that U.S. information systems are resilient against mechanical breakdown and protected against a wide variety of mischief-makers who seek to disable information networks, whether for the mere challenge of the exercise, or for more nefarious purposes.

Strong operational relationships are necessary for the management and protection of federal networks because no single federal branch, department, or agency has the authority or resources to operate and defend the interconnected systems needed to perform government functions. Just as different elements of the government designed and built information systems for their particular needs, the authorities over these networks have evolved without conscious design or structure. The major player in government information technology is not the government at all—it is the operators of the large capacity fiber-optic networks over which the majority of federal data flows: private sector Internet service providers.

These private sector entities have invested in infrastructure improvements and technology development at a rate with which the federal government cannot compete. After years of relatively generous federal spending, the budget horizon looks ominous. According to the Congressional Budget Office,"[t]he budget deficit in fiscal year 2011 will total nearly $1.3 trillion."[1] With significant federal budget reductions, government departments and agencies that do not maintain strong operational relationships with government and non-governmental partners will be overwhelmed by resource constraints, will mismanage the operation and protection of their networks, and will put other systems at risk because of the interconnected nature of information systems.

---

[1] *The History and Drivers of our Nation's Debt and Its Threats: Hearing Before the Joint Select Comm. on Deficit Reduction*, 112th Cong. 56 (2011) (prepared statement of Douglas W. Elmendorf, Director, Congressional Budget Office) (At 8.5 % of GDP, this year's deficit will be the third-largest shortfall in the past sixty-five years, exceeded only by those in 2009 (at 10.0 %) and 2010 (at 8.9 %)).

Funding constraints are one reason for strong cyber operational relationships, but the need for visibility into the health and status of government networks is another. Multiple federal systems may be linked together, but only the department, agency, or private sector owner has the ability to monitor, identify, and understand the performance of their respective networks. Shared situational awareness enables the rapid identification of malicious activity or unauthorized access across all systems. A threat to a small private sector Internet service provider may also become a threat to large federal entities because of the nature of the Internet. A threat to one is now a threat to all. Without trusted operational cyber-relationships within the federal government and between the government and private sector, adequate cyber threat information sharing will not happen.

Even with robust operational relationships, a detrimental cyber event may still occur. If a cyber event disrupts the provision of government services to the U.S. population, these functions must be restored and the loss of connectivity mitigated as quickly as possible. Hurricane Katrina provided dramatic lessons of the importance of interagency coordination and operational relationships during crises that cause widespread chaos, destruction, and communication outages. The weaker the relationships among federal departments and agencies and between the government and the private sector, the longer mitigation will take, and the more the problems will be widespread.

A natural disaster or mechanical failure may challenge the government's cyber coordination abilities, but a traditional military crisis would rapidly overwhelm an unprepared government. Although it is unlikely that a cyber attack would stand alone as a single adversarial action against the United States, the speed and distributed nature of such an attack would require close coordination between the public and private sectors, and within the national security bureaucracy. It is likely that information network capabilities would be used to nullify the conventional advantage of the U.S. military. The unique characteristics of cyber attacks[2] require operational

[2] *See* Jonathan Masters, *Confronting the Cyber Threat*, COUNCIL ON FOREIGN RELATIONS (2011), *available at* http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577. First, they are often asymmetric, meaning that actors with limited financial or technical resources have the capability to compromise high-value targets. Second, offense has the advantage in the digital realm. The web's collaborative nature means openness is prioritized over security. This design feature ensures cyber defenses lag behind offensive methods. Finally, investigations into cyber attacks suffer from a so-called attribution problem.

relationships that are agile, innovative, and do not only respond to threats quickly, but also anticipate potential adversarial actions and coordinate responses before U.S. national interests are damaged or destroyed.

Close federal cyber relationships are necessary because of the limited cyber authorities of each department and agency, the limited resources available to these departments and agencies to operate independent networks, the need for shared informational awareness, and the need for coordinated responses to foreign cyber threats. This article characterizes the operational relationships among federal government organizations with significant cyber security roles. It describes the strengths and weaknesses of those relationships and makes recommendations as to how to improve the cooperation and collaboration within the federal government. The relationships between the public sector and the private sector are then examined with descriptions of their strengths and weakness. The article concludes with recommendations for enhancing the effectiveness of these relationships.

II. FEDERAL INTERAGENCY CYBERSECURITY OPERATIONAL RELATIONSHIPS

The Government Accountability Office (GAO) has regularly designated federal information security as a high-risk area since 1997.[3] High-risk designations are for programs that are determined to have serious weaknesses, while involving significant resources and providing important public services. According to GAO:

> Executive branch agencies, in particular DHS, also need to improve their capacity to protect against cyber threats by, among other things, advancing cyber analysis and warning capabilities, acquiring sufficient analytical and technical capabilities, developing strategies for hiring and retaining highly qualified cyber analysts, and strengthening the effectiveness of the public-private sector partnerships in securing cyber critical infrastructure.[4]

---

[3] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-278, REPORT TO CONGRESS HIGH RISK SERIES: AN UPDATE 101 (2011), *available at* http://www.gao.gov/new.items/d11278.pdf.

[4] *Id.* at 102.

The departments with the largest cybersecurity budgets are the departments of Defense and Homeland Security. "For fiscal year 2012, the two [departments] requested a combined $3.4 billion in cyber-related funds (yet to be approved)."[5] The cooperation between these departments was formalized in a memorandum of agreement in September 2010 permitting the exchange of personnel to facilitate communication of each department's priorities and improve information sharing.[6] Relationships between the Federal Bureau of Investigation and the private sector have also improved with the establishment of the National Cyber Investigative Joint Task Force, which aims to "coordinate, integrate, and share information related to all domestic cyber threat investigations."[7] The task force includes eighteen intelligence and law enforcement organizations working to anticipate and prevent future cyber exploitations and to investigate the sources of illicit network activities. However, despite this progress, there are a number of challenges to effective federal interagency operational relationships in cybersecurity.

A. CHALLENGES TO FEDERAL OPERATIONAL RELATIONSHIPS

First, the federal government is very large. With a total budget of over $3.5 trillion in 2010, the federal government dwarfs the size of any private sector organization. According to the Bureau of Labor Statistics, the federal government is the largest employer in United States.[8] It is divided into three branches with unequal percentages of the federal workforce. The legislative branch is the smallest, employing approximately one percent of the federal workforce. The judicial branch is next, employing two percent. Far outpacing the other branches, the executive branch employs approximately ninety-seven percent of the federal civilian workforce (excluding Postal

---

[5] Masters, *supra* note 2.

[6] *See* Memorandum of Agreement Between the Dep't of Homeland Sec. and the Dep't of Def. Regarding Cybersecurity (Sept. 27, 2010), *available at* http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

[7] *See National Cyber Investigative Joint Task Force*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/investigate/cyber/ncijtf (last visited Feb. 17, 2012).

[8] BUREAU OF LABOR STATISTICS, U.S. DEP'T OF LABOR, CAREER GUIDE TO INDUSTRIES, 2010-11 EDITION, *available at* http://www.bls.gov/oco/cg/cgs041.htm (last visited Mar. 28, 2012) (The federal government employs approximately two million people).

Service workers).[9] Each of the federal branches, departments, and agencies has at least one network it uses to communicate and to execute its responsibilities.

Second, exact statistics on how many networks are operated by the federal departments are difficult to find.[10] This makes knowing how many connections exist between the Internet and government networks difficult to estimate. The Department of Homeland Security oversees the management of an unknown number of civilian executive branch networks. The Department of Defense oversees the management of 15,000 military networks.[11] The number of connections between different networks is determined by the nature of the network, the transactions supported by the network, the in-house applications on different networks, and data-flow efficiencies. Thus, there may be a single connection or multiple connections between any two individual networks. Under the Trusted Internet Connections initiative announced in November 2007, the Office of Management and Budget sought to standardize and secure links between individual federal networks and external, non-federal networks—including the Internet.[12] In January 2008, the number of these connections was reported to be more than 4,300.[13] If each of these connections is estimated to be associated with only ten networks—a conservatively low number—then the department would be responsible for operating and defending more than 43,000 networks.

---

[9] *Id.*

[10] A network is the entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. This is an adaptation of the definition provided by the Department of Defense. JOINT CHIEF OF STAFF, DEP'T OF DEFENSE, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 161, JP 1-02 (2012), *available at* http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (defining information system).

[11] William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy,* FOREIGN AFF., Sept./Oct. 2010, at 98.

[12] *See* Memorandum from Clay Johnson III, Office of Mgmt. & Budget, Executive Office of the President, to the Heads of Executive Dep'ts & Agencies, (Nov. 20, 2007), *available at* http://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2008/m08-05.pdf.

[13] DEP'T OF HOMELAND SEC., TRUSTED INTERNET CONNECTIONS (TIC) INITIATIVE: STATEMENT OF CAPABILITY EVALUATION REPORT 2 (2008) *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/2008_TIC_SOC_EvaluationReport.pdf.

The Department of Defense has described in great detail the information systems for which it is responsible. According to the former Deputy Secretary of Defense:

> Information technology enables almost everything the U.S. military does: logistical support and global command and control of forces, real-time provision of intelligence, and remote operations. Every one of these functions depends heavily on the military's global communications backbone, which consists of 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries. More than 90,000 people work full time to maintain it. In less than a generation, information technology in the military has evolved from an administrative tool for enhancing office productivity into a national strategic asset in its own right. The U.S. government's digital infrastructure now gives the United States critical advantages over any adversary, but its reliance on computer networks also potentially enables adversaries to gain valuable intelligence about U.S. capabilities and operations, to impede the United States' conventional military forces, and to disrupt the U.S. economy.[14]

The U.S. government remains configured in an Industrial Age structure. There have been incremental advancements in the use of information technology, but these changes have been institutionalized in isolated contexts without regard for the benefits of a unifying strategic vision. Our current circumstances present evolving and exponentially increasing cyber threats to federal systems, including unauthorized access to personally identifiable information,[15] data theft or exploitation, unauthorized access to government data, and cyber and financial crimes.

---

[14] Lynn, *supra* note 11, at 98.

[15] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-536 1, PRIVACY: ALTERNATIVES EXIST FOR ENHANCING PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (2008), *available at* http://www.gao.gov/new.items/d08536.pdf (Personally identifiable information includes any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.).

Broad changes to the structures within federal branches, departments, and agencies are unlikely. In order to maximize the efficiencies and capability of individual federal systems, strong operational relationships are necessary. The government has established some operational relationships among federal entities with cybersecurity responsibilities, and there is limited effort to improve collaboration and information sharing with the private sector.

Through intelligence and law enforcement activities, and the knowledge needed to merely operate large information networks, the federal government has extensive data about the status of individual networks, malicious activity on these networks, and the criminal activity that may be facilitated through these networks. Information sharing is necessary to capitalize on its value and produce understanding. After the attacks of September 11, 2001, the 9/11 Commission stated, "[t]he U.S. government has access to a vast amount of information. When databases not usually thought of as 'intelligence,' such as customs or immigration information, are included, the storehouse is immense."[16] The same may be said for cyber threat information. "The biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systemic resistance to sharing information."[17]

Anxiety over the loss of prosecutorial advantage, the compromise of intelligence sources and methods, and civil liability for the private sector has precluded the sharing of information among federal branches, department, and agencies—and between the government and the private sector.

> While investment banks, defense contractors, and other critical infrastructure owners have information about intrusions into their own systems and networks, they fear enforcement actions by regulators, suits by plaintiffs' lawyers, and criticism associated with public disclosure of security failures. Concerns such as these make these private entities reluctant to share information with the federal government. While federal agencies know that their networks should be protected in many of the same ways that private sector networks

---

[16] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 416-17 (2004).

[17] *Id.*

> are, concerns—including the opposition of privacy advocates to technology that sniffs traffic in and out of government systems—have slowed progress.[18]

Fear of the loss of departmental resources and authority, and the perceived need to control information in and about federal agencies, encourages unilateral approaches to federal network operations and defense. The Center of Strategic and International Studies reported on the unsatisfying progress in U.S. cybersecurity:

> Unsurprisingly, protecting "turf" played a role [in slowing cybersecurity progress]. Cyber functions are scattered across the executive branch. Reorganization could mean that some offices would have to surrender control. The different offices argue that this would put important equities that they now oversee at risk. Turf concerns intertwine with the conceptual dispute over innovation, economics, and the nature of the Internet. The cabinet agencies also have little interest in supporting a stronger White House role in cybersecurity, as it would diminish their independence.[19]

The incremental efforts made by the government are necessary but remain insufficient, particularly when cyber threats are increasingly sophisticated and numerous, and when it is likely that federal funds will be significantly reduced. According to former Defense Department official Franklin Kramer, although the current efforts to improve federal cybersecurity are welcome, "an integrated governmental strategy to meet that challenge has only begun and has yet fully to take shape."[20] Operational relationships are not yet mature enough to adequately address the loss of resources, the loss or

---

[18] Gus P. Coldebella & Brian White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. OF NAT'L SECURITY L. AND POL'Y 233, 236-37 (2010).

[19] CTR. FOR STRATEGIC AND INT'L STUDIES, COMM'N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, CYBERSECURITY TWO YEARS LATER 4 (2011), *available at* http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

[20] FRANKLIN D. KRAMER, ATLANTIC COUNCIL, CYBER SECURITY: AN INTEGRATED GOVERNMENTAL STRATEGY FOR PROGRESS (2010), *available at* http://www.acus.org/files/publication_pdfs/403/Cyber%20Security-%20An%20Integrated%20Governmental%20Strategy%20for%20Progress.pdf.

corruption of data, or the unauthorized access to national security systems caused by inadequate network security measures. Government defense contractors continue to lose terabytes of data, U.S. critical infrastructure remains unprotected, and operational relationships are not strong enough to engender trust among federal organizations and between the public and private sectors.

The remaining sections of this article will describe the cybersecurity roles and missions of some of the departments and agencies within the executive branch. Descriptions of their relationships with other parts of the government will be followed by recommendations as to how to improve these relationships for better cybersecurity for the United States.

III. DEPARTMENT OF HOMELAND SECURITY

Established by the Homeland Security Act of 2002, the Department of Homeland Security assimilated more than twenty-two federal agencies to better protect the United States from terrorism.[21] The department has multiple cybersecurity budget lines and activities. Two of the most active organizations within DHS reside within the National Protection and Programs Directorate.

The Office of Infrastructure Protection coordinates terrorism risk-reduction efforts for U.S. critical infrastructure.[22] It requested $322.3 million for fiscal year 2012 operations.[23] Within this office is the Office of Cybersecurity and Communications, which oversees the "security, resiliency, and reliability of the nation's cyber and communications infrastructure."[24] The department requested $614.2 million in fiscal year 2012 operations.[25]

---

[21] *See* Homeland Security Act of 2002, Pub. L. No. 107-296, § 101. In general, the primary mission of the Department is to (1) prevent terrorist attacks within the United States; (2) reduce the vulnerability of the United States to terrorism; and (3) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States.

[22] *About the National Protection and Programs Directorate*, DEP'T OF HOMELAND SEC. (Aug. 26, 2011), http://www.dhs.gov/xabout/structure/editorial_0794.shtm.

[23] DEP'T OF HOMELAND SEC., CONGRESSIONAL BUDGET JUSTIFICATION 1987 (2011), *available at* http://www.dhs.gov/xlibrary/assets/dhs-congressional-budget-justification-fy2012.pdf.

[24] KRAMER, *supra* note 20.

[25] Homeland Security Act of 2002, *supra* note 21.

This funding and probably more, is meant to safeguard domestic cyberspace. Other items within this budget include: $233.6 million to accelerate EINSTEIN 3[26] deployment to prevent and detect intrusions on computer systems, and to upgrade the National Cyber Security Protection System, building an intrusion detection capability and analysis capabilities to protect federal networks; $40.9 million to support the department's efforts to strengthen federal network security of large and small agencies by conducting an estimated sixty-six network assessments to improve security across the federal executive branch; $24.5 million to provide high-quality, cost-effective virtual cybersecurity education and training to develop a robust cybersecurity workforce; $1.3 million to enable DHS to coordinate national cybersecurity operations and interface with the U.S. Department of Defense's (DoD) National Security Agency (NSA) at Fort Meade, Maryland; and $18 million for the Comprehensive National Cybersecurity Initiative to support research and development projects focused on strengthening the nation's cybersecurity.[27]

The department's budget request for cybersecurity activities is large because DHS has such broad responsibilities in protecting the nation's cyber and critical infrastructure. The Secretary of Homeland Security is responsible for "coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States" and serves "as the principal federal official to lead, integrate, and coordinate implementation of efforts among federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources."[28] Although Homeland Security Presidential Directive 7 (HSPD 7) acknowledges that other departments and agencies have

---

[26] *See generally* Gov't Accountability Office, GAO-11-881, Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11 136 (2011), *available at* http://www.gao.gov/new.items/d11881.pdf. (EINSTEIN 3 is intended to be an intrusion prevention system that is to automatically detect and respond appropriately to cyber threats before harm is done.).

[27] *See generally* DEP'T OF HOMELAND SEC., FY 2012 BUDGET IN BRIEF 11-12 (2012), *available at* http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf.

[28] DEP'T OF HOMELAND SEC., HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 7 (2003) [hereinafter HSPD 7], *available at* http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

cybersecurity roles, the Department of Homeland Security is the "focal point for the security of cyberspace" for the federal government.[29]

In its first Quadrennial Homeland Security review, DHS described its mission to secure cyberspace by preventing malicious actors from "effectively exploit[ing] cyberspace, impair[ing] its safe and secure use, or attack[ing] the Nation's information infrastructure."[30] To achieve this goal, DHS must "[i]dentify and evaluate the most dangerous threats to federal[,]civilian[,] and private-sector networks and the Nation;" "[p]rotect and make resilient information systems, networks, and personal and sensitive data;" "[p]revent cyber crime and other malicious uses of cyberspace;" "[d]isrupt the criminal organizations and other malicious actors engaged in high-consequence or wide-scale cyber crime;" "[d]evelop a robust public-private cyber incident response capability;" and "[m]anage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action."[31]

To manage its broad role, the Department of Homeland Security has developed a set of guiding principles to focus the nation's response to various potential events. This National Response Framework[32] contains multiple incident annexes that address "specific contingency or hazard situations or an element of an incident requiring specialized application of the Framework."[33]

The Cyber Incident Annex describes the responsibilities of different governmental groups to "prepare for, respond to, and recover from any cyber-related Incident of National Significance

---

[29] *Id.* ("To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission.").

[30] DEP'T OF HOMELAND SEC., QUADRENNIAL HOMELAND SECURITY REVIEW 54 (2010), *available at* http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

[31] *Id.* at 55-56.

[32] DEP'T OF HOMELAND SEC., NATIONAL RESPONSE FRAMEWORK (2008), *available at* http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

[33] *See* FED. EMERGENCY MGMT. AGENCY, *National Resource Center Incident Annexes*, http://www.fema.gov/emergency/nrf/incidentannexes.htm (last visited Mar. 28, 2012) (The current annexes are: Biological Incident, Catastrophic Incident, Food and Agriculture Incident, Mass Evacuation, Nuclear/Radiological Incident, Cyber Incident, Terrorism Incident Law Enforcement and Investigation.).

impacting critical national processes and the national economy."[34] A "cyber-related Incident of National Significance" is undefined, but may include an "organized cyber attack," a widespread computer virus, a "natural disaster with significant cyber consequences," or other incidents "capable of causing extensive damage to critical infrastructure of key assets."[35] The Annex outlines the roles and responsibilities of federal departments categorized as "Coordinating Agencies, Cooperating Agencies, and Other Federal Entities."[36] In the event of a nationally significant cyber-related incident, the Department of Defense, the Department of Homeland Security, and the Department of Justice are coordinating agencies and the Departments of Commerce, Energy, Homeland Security, State, Transportation, and Treasury are all cooperating agencies.[37]

In addition to the National Response Framework's Cyber Incident Annex, DHS has drafted the National Cyber Incident Response Plan to establish the "framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident."[38] This plan is intended to expand upon the information within the NRF's Cyber Incident Annex. This plan has been in coordination for more than eighteen months and has yet to be approved by the Executive Office of the President.

---

[34] DEP'T OF HOMELAND SEC., CYBER INCIDENT ANNEX CYB-2 (2004), *available at* http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf.

[35] *Id.*

[36] *See generally* FED. EMERGENCY MGMT. AGENCY, NATIONAL RESPONSE FRAMEWORK, EMERGENCY SUPPORT FUNCTION ANNEXES: INTRODUCTION (2008), *available at* http://www.fema.gov/pdf/emergency/nrf/nrf-annexes-all.pdf (Federal agencies designated as *coordinating agencies* are responsible for implementation of processes detailed in the annexes. Coordinating agencies support the Department of Homeland Security (DHS) incident management mission by providing the leadership, expertise, and authorities to implement critical and specific aspects of the response. In accordance with Homeland Security Presidential Directive 5, DHS retains responsibility for overall domestic incident management. (Sup i); *Cooperating agencies* are those entities that have specific expertise and capabilities to assist the coordinating agency in executing incident-related tasks or processes. When the procedures within a Support Annex are needed to support elements of an incident, the coordinating agency will notify cooperating agencies of the circumstances (Sup ii).).

[37] The Intelligence Community, the National Institute of Standards and Technology, and the Office of Management and Budget are also listed as cooperating agencies.

[38] DEP'T OF HOMELAND SEC., NATIONAL CYBER INCIDENT RESPONSE PLAN, INTERIM VERSION, 1 (2010).

Despite the progress made by DHS with the as-yet-unapproved National Cyber Incident Response Plan and the cyber annex to the National Response Framework, the operational relationships between DHS and other federal departments and agencies remain underdeveloped. DHS's National Cybersecurity and Communications Integration Center (NCCIC) does not detail personnel to operations centers maintained by the Department of Defense.[39] There is limited cooperative training between the DoD and DHS for cybersecurity personnel and there is limited information sharing between the two departments, despite the memorandum of agreement signed by the secretaries of both departments.

DHS's National Cyber Security Division within the Office of Cybersecurity and Communications created the U.S. Computer Emergency Readiness Team (US-CERT) in 2003 to secure federal information networks by coordinating the "defense against and response to cyber attacks."[40] It is the federal government's focal point for interaction with executive branch and nonfederal entities on computer network "analysis, warning, information sharing, major incident response, and national-level recovery efforts." According to the Government Accountability office:

> [US-CERT] is charged with aggregating and disseminating cybersecurity information to improve warning of and response to incidents, increasing coordination of response information, reducing vulnerabilities, and enhancing prevention and protection. In addition, the organization is to collect incident reports from all federal agencies and assist agencies in their incident response efforts. It is also to accept incident reports when voluntarily submitted by

---

[39] National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 center responsible for the production of a common operating picture for cyber and communications across the federal, state, and local government, intelligence and law enforcement communities and the private sector. The NCCIC is operated within DHS' Office of Cybersecurity and Communications, a component of the National Protection & Programs Directorate. *About the National Cybersecurity and Communications Integration Center (NCCIC)*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/xabout/structure/gc_1306334251555.e (last visited Mar. 28, 2012).

[40] DEP'T OF HOMELAND SEC., OFFICE OF INSPECTOR GEN., U.S. COMPUTER EMERGENCY READINESS TEAM MAKES PROGRESS IN SECURING CYBERSPACE, BUT CHALLENGES REMAIN 2 (2010) [hereinafter GAO, CHALLENGES REMAIN], *available at* http://www.oig.dhs.gov/assets/Mgmt/OIG_10-94_Jun10.pdf.

> other public and private entities and assist them in their response efforts, as requested.[41]

US-CERT is a federal entity independent from the more than 250 global emergency teams addressing cyber incidents, including the CERT® Coordination Center (CERT/CC) at Carnegie Mellon's Software Engineering Institute.[42] US-CERT does not have the statutory or regulatory authority to enforce compliance with its notices for mitigation of cyber threats. Additionally, according to the DHS Inspector General, "US-CERT does not have sufficient staff to perform its 24x7 operations as well as to analyze security information timely."[43]

Its operational relationships with federal departments and agencies and the private sector is hindered because of inadequate information sharing based on security classification, network configuration, and training issues. Other federal agencies claim that US-CERT is "unable to share near real-time data and classified and detailed information to address security incidents."[44] Additionally, the different networks operated by other departments and the intelligence community challenge information sharing from US-CERT. Because of classification limitations, US-CERT is limited in the information it can post to its portals. Many agencies do not have classified networks or secure facilities or personnel with the proper clearances to receive the information.

DHS operational relationships would be improved if the department had a strategy to achieve its cybersecurity roles and missions. Other departments and agencies publish strategies to help communicate their priorities and initiatives. But DHS's Office of Cybersecurity and Communications has not developed "a strategic

---

[41] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-588, CYBER ANALYSIS AND WARNING: DHS FACES CHALLENGES IN ESTABLISHING A COMPREHENSIVE NATIONAL CAPABILITY 14-15 (2008), *available at* http://www.gao.gov/new.items/d08588.pdf.

[42] *See About Us*, US-CERT, http://www.us-cert.gov/aboutus.html (last visited Jan. 23, 2012) (The first of these types of organizations was the CERT Coordination Center (CERT/CC), established at Carnegie Mellon University in 1988. When the Department of Homeland Security (DHS) created US-CERT, it called upon the CERT/CC to contribute expertise for protecting the nation's information infrastructure by coordinating defense against and response to cyber attacks. Through US-CERT, DHS and the CERT/CC work jointly on these activities.).

[43] GAO, CHALLENGES REMAIN, *supra* note 40, at 7.

[44] *Id.* at 12.

implementation plan that outlines its responsibilities or establishes specific objectives and milestones for enhancing cybersecurity or protecting critical infrastructures."[45]

To improve the ability to work with other federal departments and agencies, DHS should obtain the authority to enforce guidance from US-CERT, recruit and retain adequate staff to fulfill US-CERT's mission, and establish a strategic implementation plan documenting its priorities to secure federal civilian information networks and critical infrastructures. Combined training programs with other departments and agencies would also help build operational relationships and camaraderie needed for effective communication. If implemented, these recommendations would put DHS on the road to improved collaboration and better information sharing with other parts of the federal government.

A. SECRET SERVICE

Reporting directly to the Secretary of Homeland Security, the Secret Service is responsible for safeguarding the U.S. financial infrastructure in order to "preserve the integrity of the economy, and to protect national leaders, visiting heads of state and government, designated sites and National Special Security Events."[46] The USA Patriot Act required the Secret Service to establish an Electronic Crimes Task Force in order to prevent, detect, mitigate, and investigate attacks on U.S. financial systems and critical infrastructures. The establishment of the task force was prescient considering the impact on the Dow Jones Industrial Average after a trading algorithm malfunctioned in May 2010[47] and the February 2011 cyber attack against NASDAQ OMX Group, Inc. The NASDAQ attack

---

[45] DEP'T OF HOMELAND SEC., OFFICE OF INSPECTOR GEN., PLANNING, MANAGEMENT, AND SYSTEMS ISSUES HINDER DHS' EFFORTS TO PROTECT CYBERSPACE AND THE NATION'S CYBER INFRASTRUCTURE (Redacted) 9 (2011), *available at* http://www.oig.dhs.gov/assets/Mgmt/OIGr_11-89_Jun11.pdf.

[46] U.S. SECRET SERV., U.S. DEP'T OF HOMELAND SEC., UNITED STATES SECRET SERVICE STRATEGIC PLAN (FY 2008 - FY 2013) 2 (2008), *available at* http://www.secretservice.gov/usss_strategic_plan_2008_2013.pdf.

[47] *See generally* Alex Eichler, *Lessons From the Algorithm-Fueled May 6 Flash Crash*, THE ATLANTIC WIRE (October 4, 2010), http://www.theatlanticwire.com/business/2010/10/lessons-from-the-algorithm-fueled-may-6-flash-crash/22813.

was serious enough to eventually involve the National Security Agency and the Federal Bureau of Investigation.[48]

The popularity and proliferation of information technology has enabled criminals to target financial systems, "compelling the involvement of the Secret Service in combating cyber crime."[49] The unauthorized access into NASDAQ OMX—a global exchange company—resulted in the insertion of "suspicious files" onto NASDAQ servers. Although commodities trading systems were unaffected, the intruders accessed cloud applications containing data stored by a significant number of Fortune 500 companies and providing access to "a rich mine of market-moving, inside information."[50] There is a clear role for a strong organizational element to monitor and protect U.S. financial systems against cyber criminals, hackers, and state competitors.

Also within the Secret Service is the National Threat Assessment Center (NTAC), which provides assessments "within the Secret Service and to its law enforcement and public safety partners." This organization researched "illicit insider cyber activity" because this type of activity often involves criminal activity such as "financial fraud, computer fraud, electronic crimes, identity theft, and computer-based attacks on the nation's financial, banking and telecommunications infrastructures."[51] Partnering with Carnegie Mellon University's CERT® Coordination Center, NTAC examined past instances in which current or former employees or contractors harmed their organizations "via a computer or system/network for purposes of intellectual property theft, fraud, and acts of sabotage." NTAC's study identified physical, social, and online activity that indicates an insider threat. The report identified behaviors in the

---

[48] *See generally* Uri Friedman, *Why the Financial World Is Spooked by Nasdaq Cyber Attack*, THE ATLANTIC WIRE (February 7, 2011), http://www.theatlanticwire.com/business/2011/02/why-the-financial-world-is-spooked-by-nasdaq-cyber-attack/21203.

[49] *About the U.S. Secret Service Electronic Crimes Task Forces,* U.S. SECRET SERV., http://www.secretservice.gov/ectf_about.shtml (last visited Jan. 23, 2012).

[50] *See generally* Philip Stafford, Jeremy Grant and Telis Demos, *Hacking Fears Raised by Nasdaq OMX Attack*, FIN. TIMES, Feb. 7, 2011, *available at* http://www.ft.com/intl/cms/s/0/0638d37a-32fa-11e0-9a61-00144feabdc0.html#axzz1VholGhLQ (listing financial exchanges targeted for computer attacks since 1999).

[51] *National Threat Assessment Center*, U.S. SECRET SERV., http://www.secretservice.gov/ntac.shtml (last visited Jan. 23, 2012).

banking and financial sector, the information technology and telecommunications sector, and the government sector.[52]

The Secret Service has informational awareness into systems that might not be the traditional vectors of a cyber attack. Its relationships with the private financial sector make the Secret Service the best candidate to share information from and with the financial services industry. With the ability to deal with sensitive and classified information, it does not face some of the challenges as do other Department of Homeland Security elements such as US-CERT. DHS should better leverage the Secret Service to gain better visibility into the status of network operations and malicious activity known by the financial industry. This is an example of a public-private partnership that can have significant results with little budgetary or manpower investment.

IV. JOINT COORDINATION ELEMENT

In September 2010, the Department of Homeland Security and the Department of Defense established a memorandum of agreement under which both departments will "provide personnel, equipment, and facilities in order to increase interdepartmental collaboration in strategic planning for the nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities."[53] The memorandum established a Joint Coordination Element to improve "joint operational planning, coordination, synchronization, requirement translation, and other DHS mission support for homeland security for cybersecurity" under the direct supervision of the [DHS] Director, Cybersecurity Coordination.[54] The Joint Coordination Element is the best vehicle for departmental collaboration, but remains understaffed and underutilized.

Testimony by Philip Reitinger, then the Deputy Undersecretary of the National Protection and Programs Directorate before the Senate Homeland Security Committee, in May 2011 strongly implied that the Joint Coordination Element remained long on promises and short on

---

[52] *See id.* for the actual reports and findings.

[53] *Memorandum of Agreement to Enhance Coordination to Secure America's Cyber Networks*, DEP'T OF HOMELAND SEC. (July 22, 2011), http://www.dhs.gov/files/publications/gc_1286986004190.shtm.

[54] DEP'T. OF DEF. AND DEP'T OF HOMELAND SEC., *supra* note 6.

accomplishments. He stated that, while the DoD had "unparalleled technical expertise and cyber security expertise built up over the course of years," DHS has expertise in the interagency process.[55] Reitinger noted that DHS *will be* developing people to send to the National Security Agency's (NSA) Threat Operations Center (NTOC). He noted that the National Cybersecurity and Communications Integration Center (NCCIC) *will* accept personnel from NSA and the United States Cyber Command, suggesting that individuals have yet to be integrated into this cyber watch center. The Joint Coordination Element thus remains a promising collaborative concept that has yet to be fully leveraged for the benefit of U.S. cybersecurity.

The interdepartmental agreement identified an often-overlooked element of cybersecurity: cyber acquisition. Given Moore's Law[56] and the rapid pace of technology development, traditional federal acquisition practices are insufficient. The inadequacy of DoD cyber acquisition practices was noted in the National Defense Authorization Act for fiscal year 2011.[57] This act required "a strategy to provide for the rapid acquisition of tools, applications, and other capabilities for cyber warfare for the United States Cyber Command and the cyber operations components of the military departments."[58] The agreement between the two departments acknowledges this need by requiring DHS to send personnel to the National Security Agency to collaborate on acquisition and technology development. This is another promising initiative that has yet to produce any public result.

The Joint Coordination Element is a good first step for improved collaboration and a strong operational relationship between the two departments with the largest cyber- responsibilities and the largest

---

[55] *Obama Administration Global Cybersecurity Plan: Hearing Before the Senate Homeland Security and Governmental Affairs Committee*, 112th Cong. (May 11, 2011), as seen on C-SPAN, *available at* http://c-spanarchives.org/videoLibrary/clip.php?appid=600013415.

[56] *See* DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 294-95 (1999) (For the past several decades, the number of transistors that can be placed on a single [micro processing] chip has approximately doubled every eighteen months owing to advances in manufacturing. The effect has been a corresponding doubling of processing speed in instructions per second and memory capacity in bytes per chip, with a factor of 100 improvements every five years and a factor of 100 improvements every decade. This phenomenon is called Moore's law, after the founder of and chairman of Intel, Gordon Moore, who first observed and posited it.).

[57] National Defense Authorization Act for Fiscal Year 2011, Pub. L. No. 111-383, § 933.

[58] *Id.*

budgets. To realize the full potential of the JCE, both departments should make staffing the joint organization with knowledgeable personnel from each of them a high priority. Both departments may consider making a tour in the JCE a requirement for selection to particular ranks or for selection for particular positions. Both departments should consider providing more public information on the status of the Joint Element. The memorandum of agreement was a visionary first step, but now comes the true test of the commitment to the operational relationship between the departments.

V. DEPARTMENT OF DEFENSE

"As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare."[59] The 2011 National Military Strategy describes the department's perspective on cyberspace:

> Cyberspace capabilities enable Combatant Commanders to operate effectively across all domains. Strategic Command and Cyber Command will collaborate with U.S. government agencies, non-government entities, industry, and international actors to develop new cyber norms, capabilities, organizations, and skills. Should a large-scale cyber intrusion or debilitating cyber attack occur, *we must provide a broad range of options to ensure our access and use of the cyberspace domain and hold malicious actors accountable.* We must seek executive and Congressional action to provide new authorities to enable effective action in cyberspace.[60]

The Defense Department operates its own worldwide information network, known as the Global Information Grid (GIG). The GIG is a "globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support

---

[59] Lynn, *supra* note 11, at 101.

[60] NATIONAL MILITARY STRATEGY OF THE UNITED STATES OF AMERICA 2011: REDEFINING AMERICA'S MILITARY LEADERSHIP 10 (2011) (emphasis added), *available at* http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf.

personnel."[61] It includes networks and systems that are government-owned and leased from the private sector. Without these information networks, DoD would be unable to command and control its military forces, provide logistical support, provide intelligence or communicate.

DoD has an information architecture that includes "15,000 networks and seven million computing devices across hundreds of installations in dozens of countries."[62] According to the Unified Command Plan—the document describing the responsibilities of the department's combatant commands—U.S. Strategic Command is responsible for coordinating cyberspace operational planning and directing GIG operations and defense.[63] As a subordinate unified command,[64] United States Cyber Command was established in 2009 to organize, plan, and conduct activities to direct the operations and defense of specified Department of Defense information networks; to, "when directed, conduct full-spectrum military cyberspace operations" in order to enable actions in all domains; and to "ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries."[65]

---

[61] U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE DIRECTIVE 8000.01, MANAGEMENT OF THE DEPARTMENT OF DEFENSE INFORMATION ENTERPRISE 10 (2009), *available at* http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf.

[62] Lynn, *supra* note 11, at 98.

[63] *See Unified Command Plan,* U.S. DEP'T OF DEF., http://www.defense.gov/home/features/2009/0109_unifiedcommand (last updated Apr. 27, 2011) (The Unified Command Plan is a key strategic document that establishes the missions, responsibilities, and geographic areas of responsibility for commanders of combatant commands. UCP 2011, signed by President Obama on April 6, 2011, assigns several new missions to the combatant commanders.).

[64] *See* U.S. DEP'T OF DEF., *supra* note 10 (A command established by commanders of unified commands, when so authorized by the Secretary of Defense through the Chairman of the Joint Chiefs of Staff, to conduct operations on a continuing basis in accordance with the criteria set forth for unified commands. A subordinate unified command may be established on an area or functional basis. Commanders of subordinate unified commands have functions and responsibilities similar to those of the commanders of unified commands and exercise operational control of assigned commands and forces within the assigned operational area.).

[65] *United States Cyber Command Fact Sheet,* U.S. STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/Cyber_Command (last visited Mar. 31, 2012).

It has been reported that the Defense budget request for cybersecurity operations is $3.2 billion for fiscal year 2012.[66] This request will fund improved information assurance for DoD agencies and "non-information assurance initiatives that are critical to the department's cyber stance." This large funding request pays for DoD public key infrastructure, communications security, military cyber operations, cyber research and technology, and forensic analysis conducted by the Defense Cyber Crime Center.[67]

This impressive funding illustrates the priority the Department of Defense places on cybersecurity. This effort is good for national security, but DoD is but one part of the national cybersecurity establishment. The federal government must continue to improve internal government and external partner operational relationships to better address the threats and consequences of cyber conflict. More importantly, the Defense Department must make its capabilities more available for the benefit of other federal departments and agencies.

An example of how Defense Department capabilities may be applied outside of DoD agencies is the pilot program outlined by then Deputy Secretary of Defense William Lynn in June 2011. According to the American Forces Press Service, the Defense Industrial Base (DIB) Cyber Pilot involves sharing classified threat information with participating defense contractors or with the companies' Internet service providers.[68] According to Lynn, "the government will not monitor, intercept or store any private-sector communications through the program." The intelligence provided by DoD merely helps the DIB companies "to identify and stop malicious activity within their networks."[69] The Department of Homeland Security is a partner in the DIB Cyber Pilot.

This pilot program is the singular example of how DOD cyber capabilities can assist organizations outside the Defense Department. It is admittedly easier for the department to work with the defense industrial base companies with which it has had relationships for decades than to extend its protections beyond traditional defense

---

[66] Aliya Sternstein, *Pentagon Seeks $3.2 Billion for Revised Cyber Budget*, NEXTGOV.COM (Mar.24, 2011), http://www.nextgov.com/nextgov/ng_20110324_2474.php?oref=rss.

[67] *Id.*

[68] John D. Banusiewicz, *Lynn Outlines New Cybersecurity Effort,* AMERICAN FORCES PRESS SERV. (June 16, 2011), *available at* http://www.defense.gov/news/newsarticle.aspx?id=64349.

[69] *Id.*

contractors. More programs like the DIB Cyber Pilot should be developed to leverage the experience and prior investment made to mature defense cyber capabilities. Lynn made a similar claim earlier this year stating that the "DIB Cyber Pilot could serve as an example of how a larger effort aimed at protecting the nation's critical infrastructure—its power grid, transportation system, financial system and other components—might work."[70]

The DIB Cyber Pilot and the Joint Coordination Element should inform how DoD capabilities can be leveraged to protect networks beyond its own. The Department of Defense exists and is funded to protect the United States and all of the country's interests; it was not created to protect itself. The debate about how DoD capabilities can inform and assist non-DoD cybersecurity efforts should be conducted openly and frequently. According to the Center for Strategic and International Studies, "an executive order or some other presidential document to guide military and intelligence activities in protecting critical infrastructure" would be the most visible and public statement of leveraging well-developed military capability to defend the nation's networks. "Since any decision will require working with those outside the government, a highly-classified, un-releasable document, like the 2008 Comprehensive National Cyber Initiative (CNCI), will be inadequate."[71]

Despite DoD's recognized technical expertise, the general public appears resistant to allowing DoD to protect the nation by defending non-DoD information networks.[72] DoD has an image problem. "Even if existing legal authorities allow for an expanded DoD role in defending critical infrastructure, the 'perception problem' remains significant."[73] Those resistant to a larger role for the military in protecting civilian networks are motivated by concerns for civil liberties and privacy.

In a recent report, the CSIS Commission on Cybersecurity for the 44th Presidency noted, "We do not advocate changing the traditional

---

[70] *Id.*

[71] CTR. FOR STRATEGIC AND INT'L STUDIES, *supra* note 19, at 10.

[72] *See generally*, Michael Hardy &John Zyskowski, *DOD Cyber Defense Plan Draws Fire*, FEDERAL COMPUTER WEEK (June 21, 2011), http://fcw.com/articles/2011/07/25/buzz-cyber-defense-plan-panned.aspx; Declan McCullagh, *U.S. Military Wants to "Protect" Key Civilian Networks*, CNET NEWS (July 14, 2011), http://news.cnet.com/8301-31921_3-20079500-281/u.s-military-wants-to-protect-key-civilian-networks.

[73] CTR. FOR STRATEGIC AND INT'L STUDIES, *supra* note 19, at 10.

separation that exists between military and civilian functions but believe that the administration and Congress should clarify our policies and laws to allow the military to fulfill its traditional role in protecting against foreign threats. Finding a way to do this in partnership with DHS and the private sector remains a fundamental challenge for cybersecurity policy."[74] The United States cannot afford the resources to recreate the capabilities that have already been developed for the military.

DoD's approach to cybersecurity is appropriate, but weaknesses remain. These include the lack of an adequately trained and abundant cyber workforce. There are only so many trained cyber professionals available for the federal government, and only some have gone to the better-resourced Defense Department. The military has a maturing and systemic approach to developing professional specialties in cybersecurity disciplines and will mature training to produce highly-skilled network operators to defend military networks. This will contribute to the comprehensive cybersecurity of the nation if these maturing professionals rotate to other departments and agencies. DHS has far fewer analysts and cyber professionals with the same levels of security clearance as held by DoD. Without more cleared personnel, information sharing between DHS and DoD is limited. These issues illustrate the final weakness to be resolved to operationalize the DHS-DoD relationship—speed. Without a faster mechanism to share information and make decisions, with appropriately cleared and well-trained personnel, the benefits of the DHS-DoD relationship will be lost.

Beyond the need for larger numbers of skilled cybersecurity forces and professionals, the Defense Department must carefully consider the desire to overly classify specific capabilities and strategies. Cyber warfare planning would benefit if more operations could be discussed at lower levels of classification. "While there are good reasons to highly classify and compartment some cyber matters, there is such significant over-classification and compartmentation that planning and operational integration is (sic) overly difficult."[75] Some of this over-classification is based on the intelligence sources from which the Defense establishment learns its cyber threat information. The method by which the intelligence community derives this threat intelligence is highly-classified, leading to a derivative classification of the cyber countermeasures or techniques.

---

[74] *Id.*

[75] KRAMER, *supra* note 20, at 4.

A. UNITED STATES CYBER COMMAND

Within the Department of Defense there are multiple elements that participate in the department's cyber policy or operations.[76] This article focuses mainly on the operational military cyber element, United States Cyber Command. This military organization—subordinate to United States Strategic Command[77]—"plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[78]

The command is co-located with the National Security Agency (NSA) at Fort George G. Meade, Maryland. The benefits of co-locating Cyber Command with NSA have been described by General Keith Alexander, Commander of Cyber Command and the Director of NSA:

> [Former Secretary of Defense] Gates has said we can't afford to replicate the hundreds of billions of dollars that we've put into NSA to build another architecture for Cyber Command and then yet others for different government agencies. Instead, we need to leverage existing investment and work collaboratively. NSA and Cyber Command have separate staffs and operate under different authorities. The capabilities of NSA and its work force in the signals intelligence and

---

[76] *Office of the Secretary of Defense* (responsible for coordinating the memorandum of agreement with the Department of Homeland Security), *Office of the Deputy Assistant Secretary of Defense for Cyber Policy* (supports the "Under Secretary of Defense for Policy and Assistant Security Defense for Global Strategic Affairs by developing and overseeing the implementation cyber-related policies, strategies, and plans to promote stability in and ensure continued freedom of access to the global commons of space and cyber in order to achieve national security objectives." *See Office of the Deputy Assistant Secretary of Defense for Cyber Policy,* OFFICE OF THE DEPUTY ASSISTANT SEC'Y OF DEF. FOR CYBER POL'Y, http://policy.defense.gov/gsa/cp/index.aspx (last visited Feb. 22, 2012).

[77] United States Strategic Command is responsible for nuclear capabilities, space operations, global missile defense, and global command, control, communications, computers, intelligence, surveillance and reconnaissance. *See About,* U.S. STRATEGIC COMMAND, http://www.stratcom.mil/about (last visited Feb. 22, 2012).

[78] *U.S. Cyber Command Public Affairs Fact Sheet,* U.S. STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/Cyber_Command (last visited Jan. 23, 2012).

> information assurance fields are unsurpassed. This intellectual and technical capital is critical to U.S. government efforts in cyberspace. Cyber Command is a military command that draws its authorities from Title 10, but it relies on the success of real-time intelligence, which is why the decision to collocate it with NSA was not only wise, but also an imperative.[79]

Establishing the military command with NSA reflects a national security compromise between capitalizing on NSA's technical resources, the need to centralize military cyber activities, and a desire to "balance legally-defined mission boundaries between the civilian intelligence community and the military defense community."[80] The most notable difficulty with the co-location of the command and NSA is the distinction between the military Title 10 authority of the Commander for Cyber Command and the intelligence Title 50 authority of the NSA Director.[81] Some observers appear to disregard the potential authority conflicts and believe that Cyber Command's establishment is the most significant improvement for federal cybersecurity.[82]

The benefits of interagency—or at least multi-agency advanced planning cannot be overstated. "Hurricane Katrina demonstrated how after-the-event coordination and planning was both untimely and inadequate in dealing with the immediate aftermath of the disaster."[83] Delays in interagency management can have significant operational consequences not only in a natural disaster, but also in national security scenarios. Effective coordination between Cyber Command and NSA is necessary but not sufficient in the event of a national cyber

---

[79] Harrison Donnelly, *Q&A: General Keith B. Alexander*, MILITARY INFO. TECH. (2010), *available at* http://www.kmimediagroup.com/mit-home/288-mit-2010-volume-14-issue-10-november/3650-qaa-general-keith-b-alexander.html.

[80] James Barkley, Kevin Campbell & Joseph Roybal, *Interagency Coordination @ Net Speed: Recommendations to Maximize Interagency Coordination and Capabilities at U.S. Cybercom*, May 23, 2010, John F. Kennedy School of Government, Harvard University (quoting RICHARD A. CLARK & ROBERT K. KNAKE, CYBER WAR 34–44 (2010)) (on file with the author).

[81] *Id.* Title 10 refers to that part of the United States Code governing the armed forces and Title 50 governs most intelligence operations.

[82] *See* Coldebella & White, *supra* note 18, at 4.

[83] *Id.* at 25.

emergency or attack. Cyber Command must provide a priori analysis to the national security community about the resources and manpower that are required to address a significant cyber event.

B. DEFENSE INFORMATION SYSTEMS AGENCY

The Defense Information Systems Agency (DISA) is a combat support agency providing services to the U.S. military and its allies with information networks and global communications. DISA provides "joint and coalition enterprise infrastructure, information sharing services, and command and control that enable joint warfighting." Employing more than 7,300 civilian and military personnel, the agency operates and maintains military networks and integrated capabilities—including "national nuclear command capabilities."[84] It is responsible for the ".mil" network, systems engineering, and interoperability testing, including "electromagnetic spectrum planning, coordination, deconfliction, and management services" for the Defense Department.[85] DISA's appropriated budget was over $2.5 billion for fiscal year 2011.[86]

The importance of DISA's contribution to U.S. military power is often underestimated. An example of the important work done by the agency is the Network Services directorate. This organization "translates customers' long-haul network requirements into effective voice, video and data network solutions; leverages proven and emerging technologies to ensure joint interoperability, assured security and best value; evaluates technical operations; and resolves technical support issues for DoD's long-haul networks."[87] It is also responsible for the operation and maintenance of the military's unclassified network,[88] the military secret network,[89] and the various military Network Operations Centers[90] around the world.

---

[84] *Agency Mission Essential Task List*, DEF. INFO. SYS. AGENCY, http://www.disa.mil/about/ourwork.html (last visited Jan. 23, 2012).

[85] *Id.*

[86] *Defense Information Systems Agency SNAPSHOT: A Summary of Facts and Figures*, DEF. INFO. SYS. AGENCY (Apr. 2011), *available at* http://www.disa.mil/news/pressresources/agency_snapshot.pdf.

[87] DEF. INFO. SYS. AGENCY, http://www.disa.mil/ns/index.html (last visited Jan. 23, 2012).

[88] *Network, Networking Technology, Data Communication Terms, Glossary and Dictionary: NIPRNET: Non-secure Internet Protocol Router Network*, JAVVIN NETWORK

One of the priorities highlighted in the DISA Campaign Plan is the protection of "critical infrastructure in DISA and the Global Information Grid (GIG)."[91] Given the number of unauthorized intrusions into Defense Department networks, protecting military information that transits on military networks has become an operational imperative. According to DISA's Fiscal Year (FY) 2012 Budget Estimates:

> The current world environment mandates comprehensive and integrated cyber protection for this infrastructure to ensure the DoD has protected information on protected networks. The DISA is conducting a massive effort to improve the security and defense capabilities of our military networks. These include: improved sensors for intrusion detection and reporting; demilitarized zones (DMZ) security; filtering; and developing proxys to protect our core network services from internet threats.[92]

MANAGEMENT AND SECURITY, http://www.javvin.com/networkingterms/NIPRNET.html (last visited Apr. 1, 2012).

[89] *Secret Internet Protocol Router Network: (SIPRNET Network Security Plan)*, http://www.docstoc.com/docs/14976132/Secret-Internet-Protocol-Router-Network (last visited Apr. 1, 2012).

[90] The Global Network Operations and Security Center (GNOSC) provides situational awareness of the myriad of networks, systems and applications that make up the Global Information Grid (GIG) and protect/defend that grid from potential cyber threats. Additionally, the GNOSC performs a Command Center function that provides a wide variety of support to the Defense Information Systems Agency's (DISA) core mission areas.

[91] DEF. INFO. SYS. AGENCY, DISA CAMPAIGN PLAN 10 (2011-2012). The Global Information Grid is the terms once used to describe the globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (*See* Joint Publication 1-02, 154).

[92] DEF. INFO. SYS. AGENCY, FISCAL YEAR 2012 BUDGET ESTIMATES 207-08 (2012), *available at* http://comptroller.defense.gov/defbudget/fy2012/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PARTS/O_M_VOL_1_BASE_PARTS/DISA_OP-5_FY_2012.pdf.

An examination of DISA's budget request yields mixed results given the importance of network defense in a time of growing threats—particularly to military systems. DISA arranges its resources into six mission areas.[93] The "GIG Network Operations and Defense" mission area covers the operation, *protection, defense*, and sustainment of the "enterprise infrastructure and information sharing services which enable Command and Control."[94] Yet, the funding for this mission area has been reduced from $517 million in fiscal year 2011 to $445 million in fiscal year 2012.[95]

This reduction may not indicate DISA's lack of prioritizing network security, as only two of the six operations funded under GIG Network Operations and Defense resource line were actually reduced. These two missions are to ensure "critical mission execution in the face of cyber attacks"[96] and "develop and implement Cybersecurity plans, assessments, and strategies . . . ."[97] It is significant to note, however, that DISA's funding for support of the Defense Industrial Base (DIB) grew by more than $5 million from FY11 to FY12. This activity provides "information assurance/computer network defense support to the DIB through rapid dissemination of cyber threat, vulnerability, and analysis information."[98] It is "devoted exclusively to cyber indications and warning, intrusion detection, incident analysis, incident response, information sharing/knowledge management, and planning."[99]

DISA's mission is clearly critical to the overall cybersecurity of the United States. Without reliable military command and control and communications infrastructure, the ability for the U.S. to use its superior military force is diminished.

---

[93] *Id.* at 208. (Transition to Net Centric Environment, Eliminate Bandwidth Constraints, GIG Network Operations and Defense, Exploit the GIG for Improved Decision Making, Deliver Capabilities Effectively/Efficiently).

[94] *Id.* (emphasis added).

[95] *Id.* at 217. (emphasis added).

[96] *Id.* at 218.

[97] *Id.* at 219.

[98] *Id.* at 221.

[99] *Id.*

VI. NATIONAL SECURITY AGENCY AND THE INTELLIGENCE COMMUNITY

As a member of the Intelligence Community, the National Security Agency (NSA) collects, analyzes, and produces "signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions."[100] With respect to cybersecurity, the Director of NSA is also the National Manager for National Security Systems and responsible to the Secretary of Defense for the protection of national security systems.[101]

There has always been tension between operational combat commanders and the intelligence organizations that support them. According to Michael Handel:

> Intelligence is of the utmost importance in war, but it is not a prerequisite for military conflict or even victory. The best intelligence is impotent without military strength, while military strength without intelligence can nevertheless accomplish its objectives though probably at a higher cost. Consequently, military organizations have traditionally viewed the operational branch, the fighting forces, as their central concern at all times.[102]

Military commanders demand certainty and predictability. Intelligence agencies tend to deliver uncertain and qualified judgments. In a paper concerning the Intelligence Community's performance in Afghanistan, the then-Deputy Chief of Staff for Intelligence for the International Security Assistance Force in Afghanistan said that "because the United States has focused the overwhelming majority of collection efforts and analytical brainpower on insurgent groups, our intelligence apparatus still finds itself unable to answer fundamental questions about the environment in which we operate and the people we are trying to protect and persuade."[103]

---

[100] Exec. Order No. 12333 (2008).

[101] *See* 40 U.S.C. § 11103.

[102] INTELLIGENCE AND MILITARY OPERATIONS 65-66 (Michael I. Handel ed., 1990).

[103] MAJOR GENERAL MICHAEL T. FLYNN, U.S.A., CAPTAIN MATT POTTINGER & PAUL D. BATCHELOR, FIXING INTEL: A BLUEPRINT FOR MAKING INTELLIGENCE RELEVANT IN AFGHANISTAN 4 (2010), *available at* http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf.

Because NSA is an agency within the Department of Defense and because it is now co-located with a cyber combat command, there may be tensions between the operational priorities of Cyber Command and those of the NSA. Despite these potential tensions, as discussed above, there is great wisdom in co-locating Cyber Command with NSA.

The National Security Agency is the world's preeminent signals intelligence organization.[104] Not only is it responsible for the collection and analysis of foreign diplomatic, military, and commercial communications, but it also is charged with securing U.S. communications from interception. Part of the agency's mission includes enabling "Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances."[105]

An example of the cybersecurity benefits derived from NSA is the Department of Homeland Security's EINSTEIN program. Under this program, the Department of Homeland Security is partnering with an Internet service provider to test technology that detects unauthorized intrusions into government computer systems using capabilities developed by the National Security Agency.[106] The automation of this malware detection is meant to prevent attacks before damage is done to federal information systems or data is stolen or manipulated within federal databases. "EINSTEIN 3's predecessors focused on intrusion detection, allowing analysts to scan records of connections to agencies' systems and use signatures to scan network traffic for cyber threats. EINSTEIN 3 would add the ability to prevent those intrusions."[107] This effort will improve DHS's information sharing by providing an automated process for alerting other agencies about network intrusions.

As illustrated by the EINSTEIN technology, NSA and the intelligence community may have insight into the working of terrorist organizations that seek to damage U.S. interests using the Internet.

---

[104] *See generally* JEFFREY T. RICHELSON, THE U.S. INTELLIGENCE COMMUNITY 31 (4th ed., 1999). (Signals intelligence includes communications intelligence and electronic intelligence).

[105] NAT'L SEC. AGENCY, NSA/CSS STRATEGY (2010), *available at* http://www.nsa.gov/about/_files/nsacss_strategy.pdf.

[106] Ben Bain, *DHS Releases New Details on EINSTEIN 3 Intrusion Prevention Pilot*, FEDERAL COMPUTER WEEK (Mar. 19, 2010), *available at* http://fcw.com/articles/2010/03/19/einstein-3-test-intrusion-prevention-system.aspx.

[107] *Id.*

According to the Congressional Research Service, "Terrorist organizations exploit the Internet medium to raise awareness for their cause, to spread propaganda, and to inspire potential operatives across the globe. Websites operated by terrorist groups can contain graphic images of supposed successful terrorist attacks, lists and biographies of celebrated martyrs, and forums for discussing ideology and methodology."[108] The global reach and resident analytical skill of the intelligence community—including NSA—provides enormous advantage to U.S. cybersecurity.

Under the National Cyber Incident Response Plan, the intelligence community is tasked with providing advanced warning and characterization of a cyber attack. In concert with the Department of Defense, the intelligence community will "characterize the cyber threat and attribution of attacks and to forestall future incidents."[109] Intelligence agencies are also tasked with establishing situational awareness with DHS and "other partners" and to share intelligence on threats in and from cyberspace with the private sector and "especially the critical infrastructure and key resources (CIKR) community."[110]

The Department of Defense and the intelligence community operate under some distinct legal authorities however. This is both a benefit and a liability in terms of cybersecurity. According to General Alexander, a cyberspace destructive attack "is coming, in my opinion. It is a question of time." He noted that the timing of this attack is unknown and that he cannot predict if this event will be against "commercial infrastructure, government networks or mobile platforms."[111]

A cyber conflict may be inevitable, but the Defense Department does not possess the inherent legal authority or capacity to respond to all cyber threats unilaterally. As with a natural disaster, timely and effective interagency coordination is necessary to synchronize and

---

[108] CATHERINE A. THEOHARY & JOHN ROLLINS, CONG. RES. SERV., R41674, TERRORIST USE OF THE INTERNET: INFORMATION OPERATIONS IN CYBERSPACE 3 (2011), *available at* http://www.carlisle.army.mil/dime/documents/Terroist%20Use%20of%20Internet%20IO.pdf.

[109] DEP'T OF HOMELAND SEC., NATIONAL CYBER INCIDENT RESPONSE PLAN, E-1 (2010) [hereinafter NATIONAL CYBER INCIDENT RESPONSE PLAN], *available at* http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

[110] *Id.*

[111] Donna Miles, *Alexander Cites Need for Greater Cyber Defenses*, AMERICAN FORCES PRESS SERV., (Sept. 13, 2011), *available at* http://www.defense.gov/news/newsarticle.aspx?id=65321.

focus all instruments of national power against current and emerging cyber threats.[112] DoD currently has no authority to guard networks other than the GIG. Yet, threats to the U.S. may pass through multiple other networks, foreign and domestic, before putting DoD at risk. NSA can monitor foreign communications outside the U.S., but can do nothing to mitigate a threat it may see coming. Despite the technical brilliance resident at NSA, the agency and the intelligence community must develop close relationships with the Department of Homeland Security to execute a unified homeland defense strategy.

Both the Defense Department and the intelligence community must protect information systems that are required to perform their missions. Both federal elements know how to detect cyber intrusions, protect essential networks, and respond to threats to U.S. interests. According to Franklin Kramer, however, "the technical solutions for securing civilian infrastructure vulnerability and espionage are either not available or not well understood."[113] Kramer notes that the "creation of an effective technical architecture with adequate situational awareness, resilience and interoperability will be a significant challenge."[114]

The weakness of the intelligence community and NSA is cultural. The multi-billion dollar intelligence community produces the most sensitive information available to the government and, therefore, has many more personnel with higher security clearances. The military's average clearance level is still higher than that of DHS, but it still doesn't match that of an intelligence agency.

VII. DEPARTMENT OF JUSTICE

As the key source of legal guidance within the executive branch, the Justice Department is a necessary partner in U.S. cybersecurity, especially because clear laws governing some unique aspects of cybersecurity have yet to be written. For example, determining what actions against the U.S. justify retaliation is a question that the department must consider. The lack of cyber-experienced attorneys

---

[112] James Barkley, Kevin Campbell, Joseph Roybal, *Interagency Coordination @ Net Speed: Recommendations to Maximize Interagency Coordination and Capabilities* (US CYBERCOM 26, John F. Kennedy School of Government, Harvard University) (on file with author).

[113] KRAMER, *supra* note 20, at 3.

[114] *Id.*

challenges almost all branches of the department. Although there may be a sufficient number of attorneys with military experience, very few of them have military cyber experience. This limits their ability to provide guidance for and participate in discussions of cyber conflict and the emerging authorities for cyber-operational relationships. The Justice Department will have to explore, debate, and determine adequate legal guidance for a federal government that relies on information networks to provide for the U.S. population.

A. FEDERAL BUREAU OF INVESTIGATION

Criminal acts in U.S. cyberspace are addressed by the Federal Bureau of Investigation. Such acts may be politically motivated; more often, crimes such as fraud or the theft of intellectual property are motivated by the pursuit of illicit profit. Some estimate the cost of cyber crime to be in the hundreds of billions of dollars.[115] Operational relationships between the Departments of Homeland Security, Defense, and Justice are critical because "there is not necessarily a bright line between national security and criminal objectives: the well-known [December 2009] attack on Google may be an exemplar of a hybrid situation."[116]

IX. DEPARTMENT OF COMMERCE

A. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

The National Institute of Standards and Technology (NIST) is a Department of Commerce non-regulatory agency and "provides standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services."[117] NIST's Computer Security Division encourages "broad sharing of information security tools and practices," and "provides a resource for information security standards and guidelines."[118]

---

[115] *See generally* NATIONAL CYBER INCIDENT RESPONSE PLAN, *supra* note 109.

[116] *Id.*

[117] *Computer Security Resource Center*, NAT'L INST. OF STANDARDS AND TECH., http://www.nist.gov/itl/csd/csrc.cfm (last visited Jan. 23, 2012).

[118] *Id.*

NIST's Computer Security Division fulfills the institute's responsibilities under Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA).[119] Under its FISMA authorities, the Computer Security Division drafted FISMA compliance guides, "provided specifications for minimum security requirements for federal information and information systems," and reviewed "security policies and technologies from the private sector and national security systems for potential federal agency use."[120]

NIST has a vital role to play at the nexus of U.S. government and the private sector. By statute, "NIST is directed to offer support to the private sector for the development of precompetitive generic technologies[121] and the diffusion of government-developed innovation to users in all segments of the American economy."[122] Title 15 also directs NIST to "develop and test standard interfaces, communication protocols, and data structures for computer and related telecommunications systems,"[123] to "study computer systems and their use to control machinery and processes,"[124] and to "perform research

---

[119] FISMA the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide information security program. The law assigns specific responsibilities to agency heads, chief information officers, and Inspectors General. It also assigns OMB and the National Institute of Standards and Technology (NIST) with responsibilities for oversight and guidance. The Office of Management and Budget (OMB) is responsible for overseeing agency information security policies and practices, including developing and overseeing guidance on information security and overseeing compliance. NIST is tasked with developing standards and guidance for implementation of FISMA requirements by federal agencies. (*See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-528, INFORMATION SECURITY: SELECTED DEPARTMENTS NEED TO ADDRESS CHALLENGES IN IMPLEMENTING STATUTORY REQUIREMENTS (2007)).

[120] *The Computer Security Division Responds to the Federal Information Security Management Act of 2002*, COMPUTER SCIENCE DIV., NAT'L INST. OF STANDARDS AND TECH., http://csrc.nist.gov/about/index.html (last visited Jan. 23, 2012).

[121] *See generally* WENDY H. SCHACHT, CONG. RES. SERV., CRS Report 95-36, THE ADVANCED TECHNOLOGY PROGRAM 2 (2005), *available at* http://www.au.af.mil/au/awc/awcgate/crs/95-36.pdf (high-risk [research] . . . past the basic research stage but not yet ready for commercialization).

[122] WENDY H. SCHACHT, CONG. RES. SERV. CRS 95-30, THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: AN APPROPRIATIONS OVERVIEW 1 (2011), *available at* http://assets.opencrs.com/rpts/95-30_20110425.pdf; *see also* 15 U.S.C. §272(b)(1) (2010).

[123] 15 U.S.C. § 272(c)(12).

[124] *Id. at* § 272(c)(13).

to develop standards and test methods to advance the effective use of computers and related systems and to protect the information stored, processed, and transmitted by such systems and to provide advice in support of policies affecting Federal computer and related telecommunications systems."[125]

FISMA provides government-wide requirements for information security that supersede the Government Information Security Reform Act and the Computer Security Act. "Except for national security systems as defined by FISMA, the Secretary of Commerce is responsible for prescribing standards and guidelines pertaining to Federal information systems on the basis of standards and guidelines developed by NIST."[126]

NIST and the National Security Agency cooperatively evaluate information technology conformance with international standards under the National Information Assurance Partnership (NIAP). This cooperative effort is the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS). It is a public-private partnership to "help consumers select commercial off-the-shelf information technology (IT) products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace."[127]

Although NIST is a vital player in the cybersecurity game, divided authorities may hobble the federal government's ability to adequately secure essential information and critical U.S. networks. The Department of Homeland Security "working with [NIST] and [the Office of Management and Budget]—defends all '.gov' space; and DoD defends all of the '.mil' space for military and intelligence networks."[128] No federal organization helps protect commercial networks "where our policy is to rely on some combination of individual action, encouragement, leadership by example, and faith in market forces."[129]

---

[125] *Id. at* § 27(c)(14).

[126] WILLIAM C. BARKER, NAT'L INST. OF STANDARDS & TECH., GUIDELINE FOR IDENTIFYING AN INFORMATION SYSTEM AS A NATIONAL SECURITY SYSTEM 5 (2003), *available at* http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf.

[127] *Common Criteria Evaluation and Validation,* NAT'L INFO. ASSURANCE P'SHIP, http://www.niap-ccevs.org/about (last visited Jan. 23, 2012).

[128] Coldebella & White, *supra* note 18, at 7.

[129] *Id.*

X. LEGISLATIVE BRANCH

Considerations of the complexities surrounding the cybersecurity of legislative branch networks are beyond the scope of this article; however, since there are connections between the networks of both branches, a few issues should be mentioned. Given the complicated cybersecurity relationships within the executive branch, it is easy to overlook the important role the legislative branch plays in setting funding and policy for U.S. cybersecurity. According to Stephen Dycus:

> Congress obviously cannot act alone to develop a cyber warfare policy for the United States. Its members and staff lack the technical expertise, agility, and organization to wield this new, evolving weaponry. On the other hand, Congress's job in our constitutional system is to set national policy for the executive branch to execute. Especially in the matter of cyber warfare, where the diplomatic and strategic stakes are potentially as high as they are in any kinetic conflict, Congress has a critical role to play. It has perspective gained from long experience in foreign affairs and a host of related issues, and it may be more responsive to the popular will. The solution to this apparent conundrum may be found in a close collaboration between the political branches in the planning and implementation of rules for cyber warfare.[130]

Professor Dycus makes the point that U.S. cyberspace actions are still governed by law. If the nation suffers a significant cyber event that is determined to be an armed attack under the United Nations Charter, the "United States' laws and rules must govern the United States' response—and, in particular, the relationship between the executive branch and the Congress. An appropriate declaratory policy, as has been used with respect to other types of potentially serious attacks, could help create a common executive branch-congressional understanding."[131]

---

[130] Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SECURITY L. & POL'Y 155 (2010).

[131] KRAMER, *supra* note 20, at 2.

XI. NON-FEDERAL SECTOR CYBERSECURITY OPERATIONAL RELATIONSHIPS

External operational relationships are more relevant and important when the United States is faced with a potential cyber conflict. The relationships between the U.S. government and the private sector are critical because the private sector is more likely to notice a cyber attack before it affects U.S. systems. The majority of the systems and critical infrastructure on which the federal government relies are owned and operated by the private sector. Ninety-eight percent of government communications, including classified data, travel over "civilian-owned-and-operated networks and systems."[132]

According to the Intelligence and National Security Alliance, the relationship between the private sector and the federal government is insufficient to secure U.S. critical infrastructure. Government and private cybersecurity efforts remain uncoordinated, allowing malware to spread "undetected to any location benefiting from the near absence of security between independent network owners. This lack of coordination across the public and private sector leaves the user vulnerable to malevolent behavior that, among a long list of possibilities, can invade their privacy, steal their identities, deny critical services, or create conditions in which public confidence in governmental institutions is diminished."[133]

There are evolving efforts for coordination between the government and commercial sectors. Multiple advisory committees and partnerships with private industry are involved in cybersecurity. The bodies that attempt to provide stronger public-private partnerships have been less than successful, however, because there is no regulatory structure to allow adequate operational relationships between the public sector and federal departments and agencies. The Center for Strategy and International Studies points to DoD's Defense Industrial Base Cyber Pilot and the Enduring Security Framework as two of the few successful partnerships in government. Their success is

---

[132] Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1534 (2010) (quoting Michael McConnell, Former Dir. of Nat'l Intelligence, from his Keynote Address at the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology).

[133] INTELLIGENCE AND NAT'L SEC. ALLIANCE, ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS (2009), *available at* http://www.insaonline.org/assets/files/CyberPaperNov09R3.pdf.

based on the "high-level participation by all parties and the existence of binding contractual relationships."[134]

The private sector continues to struggle with the costs of improving security for its information and networks. According to Larry Clinton of the Internet Security Alliance, "Many companies don't see an adequate [return on investment] to cyber investments."[135] The lack of an adequate business case to encourage greater cybersecurity creates regulatory dilemmas. Melissa Hathaway[136] has offered three options for steepening the "demand curve for cybersecurity."[137] She recommends that the Securities and Exchange Commission propose a rule governing the thresholds of information security risk. This would demonstrate the SEC's interest in corporate information on company information security safeguards.[138]

Second, Hathaway recommends the Federal Communications Commission require the "core telecommunications providers and [internet service providers]...shoulder more of the burden of protecting our infrastructure." The private sector often tells the government that private firms are better positioned than government agencies to detect and mitigate cyber threats. If this is the case, then the government should endorse the cyber capabilities of the private sector and capitalize on the "unparalleled visibility into global networks" of the ISPs.[139]

---

[134] Coldebella & White, *supra* note 18, at 4.

[135] *Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal: Hearing Before H. Subcomm. on Cybersecurity, Infrastructure Protection, and Sec. Technologies*, 112th Cong. (2011) (testimony of Larry Clinton, President & CEO, Internet Security Alliance), *available at* http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Clinton%20Amended.pdf.

[136] President of Hathaway Global Strategies and senior adviser at the Harvard Kennedy School's Belfer Center led President Obama's Cyberspace Policy Review as National Security Council acting senior director for cyberspace. Hathaway also led the development of the Comprehensive National Cybersecurity Initiative in the Bush White House.

[137] *See generally* MELISSA HATHAWAY, ATLANTIC COUNCIL, ISSUE BRIEF: CREATING THE DEMAND CURVE FOR CYBERSECURITY (2010), *available at* http://www.acus.org/files/publication_pdfs/403/121610_ACUS_Hathaway_CyberDemand.pdf.

[138] MELISSA HATHAWAY, ATLANTIC COUNCIL, ISSUE BRIEF: CREATING THE DEMAND CURVE FOR CYBERSECURITY 2 (2010), *available at* http://www.acus.org/files/publication_pdfs/403/121610_ACUS_Hathaway_CyberDemand.pdf.

[139] *Id.* at 1.

Third, the Federal Trade Commission has appropriate authority to "protect and educate consumers and businesses on the fundamental importance of good information-security practices."[140] Through the application of a warning banner or notice message, online consumers can be informed of the risk they are assuming by conducting e-transactions. These banners are comparable "to the warning labels found on tobacco and alcohol products, telling consumers they can be hazardous to their health."[141]

In October 2011, the SEC issued guidance essentially adopting Hathaway's recommendations. The new regulation requires public companies to report "significant instances of cybertheft or attack, or even when they are at material risk of such an event."[142]

A. THE DEPARTMENT OF HOMELAND SECURITY AND THE PRIVATE SECTOR

The Homeland Security Act of 2002 assigned the following responsibilities for the protection of critical infrastructure to DHS:

- developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States;
- recommending measures to protect the key resources and critical infrastructures of the United States in coordination with other groups; and

---

[140] *Id.* at 5.

[141] *Id.*

[142] Ellen Nakashima & David S. Hilzenrath, *Cybersecurity: SEC Outlines Requirement That Companies Report Cyber Theft and Attack*, WASH. POST, Oct. 14, 2011, http://www.washingtonpost.com/world/national-security/cybersecurity-sec-outlines-requirement-that-companies-report-data-breaches/2011/10/14/gIQArGjskL_story.html; *see also* DIV. OF CORP. FIN., SEC. AND EXCHANGE COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2 CYBERSECURITY (2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

- disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of or response to terrorist attacks.[143]

DHS communicates with the private sector primarily through the Information Sharing and Analysis Centers (ISACs). In 1998, Presidential Decision Directive 63 called for the establishment of ISACs as means to assist with the protection of critical infrastructure. Yet, "[f]requent reliance on cooperative councils, like the ISACs, has produced little more than the repetitive refrain that government can't share intelligence with the private sector and the private sector sees little to gain by sharing with the government."[144]

The strength of DHS's relationship with the private sector is that DHS has provided a venue to share information, which is necessary but not sufficient. The weaknesses of this approach, however, is that it is voluntary and there is no cost to not participating. Private sector motivation for sharing information with the government is reduced by the monetary risk of releasing proprietary information to competitors and the potential liability of releasing customer date, if sued. There is also the "FOIA" risk. Private sector firms are not subject to Freedom of Information Act (FOIA) requests for information, but under the current legal regime any information provided to the government, if not subject to a FOIA exemption—national security, for example—could be released to the public.

Within DHS, the National Protection and Programs Directorate oversees the Office of the Assistant Secretary for Cybersecurity and Communications. The office uses three divisions[145] to "prevent or minimize disruptions to [U.S.] critical information infrastructure in order to protect the public, economy, government services, and the overall security of the United States." The CS&C Office seeks to reduce

---

[143] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-628 , CRITICAL INFRASTRUCTURE PROTECTION: KEY PRIVATE AND PUBLIC CYBER EXPECTATIONS NEED TO BE CONSISTENTLY ADDRESSED 7 (2010), *available at* http://www.gao.gov/new.items/d10628.pdf.

[144] Paul Rosenzweig, *The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence, in* DETERRING CYBER ATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 244, 266 (2010).

[145] *See National Communications System*, NAT'L CYBER SECURITY DIV. OFFICE OF EMERGENCY COMMC'S, http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm (last visited Feb. 2, 2012) (The three divisions are the National Communications System, the National Cyber Security Division, and the Office of Emergency Communications.).

cyber vulnerabilities, guard against cyber intrusions, and anticipate potential threats.[146]

However, according to a DHS Inspector General Report from June 2011, CS&C has not adequately addressed cybersecurity risks. The office has yet to craft a strategic implementation plan to address the recommendations from the *National Strategy to Secure Cyberspace*,[147] or to accomplish the objectives established by the National Infrastructure Protection Plan or the Comprehensive National Cyber Security Initiative. According to the IG, "Although progress has been made in building relationships with the public and private sectors, raising cybersecurity awareness, and implementing education and outreach programs, much work remains to protect cyberspace and the Nation's critical infrastructures from vulnerabilities and exploits."[148]

B. THE DEPARTMENT OF DEFENSE AND THE DEFENSE INDUSTRIAL BASE

The Defense Department has its own relationships with a small portion of the private sector known as the Defense Industrial Base. This effort provides expertise to defense contractors who have "opted-in" to the program. "Through a public-private partnership called the Enduring Security Framework (ESF), the chief executive officers and chief technology officers of major information technology and defense

---

[146] *Office of Cybersecurity and Communications,* U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm (last visited Jan. 23, 2012).

[147] *See* THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf. The *National Strategy to Secure Cyberspace* outlined a framework for both organizing and prioritizing efforts. It provides direction to the federal government departments and agencies that have roles in cyberspace security. It also identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. The *Strategy* highlights the role of public-private engagement. The document provides a framework for the contributions that we all can make to secure our parts of cyberspace. The dynamics of cyberspace will require adjustments and amendments to the *Strategy* over time. *See id.* at viii.

[148] DEP'T OF HOMELAND SEC., OFFICE OF THE INSPECTOR GEN., PLANNING, MANAGEMENT, AND SYSTEMS, ISSUES HINDER DHS' EFFORTS TO PROTECT CYBERSPACE AND THE NATION'S CYBER INFRASTRUCTURE (Redacted) 13 (2011), *available at* http://www.oig.dhs.gov/assets/Mgmt/OIGr_11-89_Jun11.pdf.

companies now meet regularly with top officials from DHS, ODNI, and DoD."[149]

The benefits of this relationship are faster identification and application of commercial best practices from top industry leaders. The ESF addresses how the "technological, operational, and political factors introduce exposure for the U.S. and opportunity for our adversaries, identify the means to manage the risk profile for the U.S. and its allies in this environment, and address today's risk and provide a permanent forum for continued engagement in tomorrow's technology marketplace."

The downsides are similar to those in the ISACs—a limited government ability to share classified information with the private sector and the private sector's limited inclination to share with government due to its proprietary concerns and liability issues. The Department has involved some of its Defense Industrial Base (DIB) contractors in a pilot program to "improve sharing of information on cyber threat, alerts, and sensitive data by establishing a new partnership model."[150] This pilot program is governed by voluntary agreements between DoD and cleared defense contractors. These contractors receive classified and unclassified cyber threat information and best practices:

> In return, the private sector partners agree to share cyber intrusion information with the DoD Cyber Crime Center, which is to serve as the focal point for information-sharing and digital forensics analysis activities related to protecting unclassified information on DIB information systems and networks. DoD's goal is to transition from pilot to program status and expand the program to all qualified cleared contractors. In addition, the officials stated that they expect to eventually modify DoD contractual language to encourage contractors to increase cybersecurity in their networks.[151]

---

[149] William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFF., Sept./Oct. 2010.

[150] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-628, CRITICAL INFRASTRUCTURE PROTECTION: KEY PRIVATE AND PUBLIC CYBER EXPECTATIONS NEED TO BE CONSISTENTLY ADDRESSED 22 (2010), *available at* http://www.gao.gov/new.items/d10628.pdf.

[151] *Id.* at 23.

XII. CONCLUSION

The federal government requires adequate operational relationships that will facilitate information and resource sharing in times of expanding cybersecurity threats and shrinking federal budgets. All federal departments and agencies must participate and contribute to more secure information systems, but the departments with the largest budgets and most expertise—the Departments of Defense and Homeland Security, and those with greater insight into the capabilities and intentions of potential adversaries—likely have the most significant contributions to make across the federal government and the private sector.

The Defense Industrial Base Cyber Pilot conducted by DoD and the EINSTEIN program initiated by DHS are excellent examples of collaboration within government and with the private sector. These initiatives require expansion and maturation. The collaborative efforts between DoD and DHS in the Joint Coordination Element need to become stronger vehicles for information sharing and cooperative planning. Following these recommendations will result in better avoidance of, preparation for, and recovery from a devastating cyber attack. The United States government has established good operational relationships to address the cyber threat, but it must improve these relationships to be more inclusive and to coordinate at a much faster pace.